玄门盾

安全SDK接入方案轻松防御DDoS/CC攻击和业务欺诈

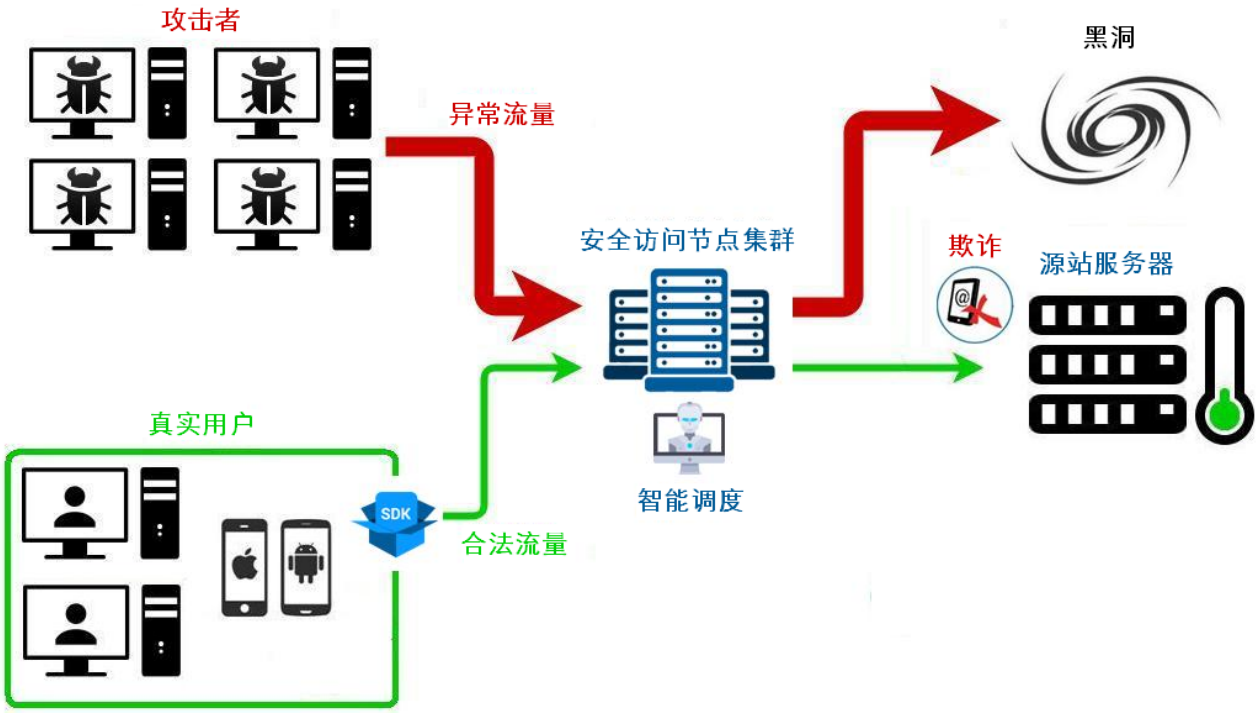
什么是玄门盾

近年来，DDoS网络攻击和业务欺诈在激烈商业竞争的推动下，不断呈现复杂化、智能化、工具化的特点，使得传统防御方式无力应对，成为互联网行业的主要威胁。

DDoS网络攻击可采用大流量的攻击方式在短时间内让服务器瘫痪，也可采用伪造合法请求的CC攻击方式来持续消耗服务器资源。防御一次DDoS/CC攻击，企业可能要使用5万倍于攻击者的流量，花费数百万人民币，攻防双方投入成本严重失衡。业务欺诈则是攻击者通过技术手段，利用盗用伪造或篡改的用户设备信息，对各类互联网服务提供商实施作弊诈骗，获取不正当利益的另一种常见方式。

针对互联网行业面临的以上威胁，玄吉科技推出了有针对性的网络/业务安全整体解决方案——玄门盾，除了可以抵御大规模的DDoS/CC攻击以外，还可有效防范业务欺诈行为，使得各类行业用户的互联网安全防护成本更低，效果更好。

玄门盾如何防护



基于玄门盾的安全SDK和加速安全访问节点集群，帮助互联网行业用户搭建起可隐藏源站服务器IP的安全防护屏障，且防护屏障可跨云部署。通过玄门盾特有的设备指纹鉴别技术和安全访问节点智能调度技术，可以将“合法流量”和“异常流量”快速甄别分流，再将“合法流量”转发到源站服务器。除了使正常用户访问不受DDoS/CC攻击影响以外，还让伪造用户行为的业务欺诈也无法奏效。

玄门盾技术优势

	玄门盾	传统防御
DNS防护	无需DNS解析，SDK分配安全访问节点的公网真实IP地址	无DNS攻击保护
DDoS/CC防护带宽	摆脱DDoS/CC攻防军备竞赛，可防御T级超大规模攻击，正常用户访问不受影响	防护带宽有限，数据清洗会导致正常用户访问性能下降 基于HTTP/HTTPS协议的攻击需要部署单独的Web防火墙，但渗透率高
设备指纹	人机识别，约200余项终端设备安全运行环境检测项目 生成唯一设备指纹ID，并标识设备信誉等级 超大规模设备指纹库	无终端设备安全运行环境检测，无设备指纹ID
业务欺诈和风控	利用设备指纹鉴别技术，可针对任何网络协议的伪造，迅速鉴别业务欺诈行为 风控覆盖移动端安全，网络安全，业务安全，大数据分析，机器学习，黑白名单，行业风控模型等多维度	依靠报文深度分析、IP信誉库、Cookie等技术，误判率和渗透率高 协议防护算法更新慢，性能差 很难支持基于TCP私有协议的防护 风控维度覆盖率低
响应速度	全网BGP，智能选取最优线路，保证网络灵活与稳定 毫秒级鉴别，实时决策，秒级智能调度，弱化用户感知	解析清洗使得用户访问响应速度明显下降

玄门盾适合哪些场景

- 适合金融，电商，游戏，媒体，O2O等各类行业用户
- 可防御T级大规模DDoS/CC攻击（例如：SYN Flood、ACK Flood、ICMP Flood、UDP Flood、空连接、慢连接、协议仿真等）
- 反欺诈业务场景
  - 注册登录：垃圾注册、代理IP、短信通道、恶意调用等
  - 营销活动：羊毛党、差评党、黄牛党、刷单、刷榜、机器秒杀、抢优惠、投票竞价作弊等
  - 渠道推广：设备牧场，刷点击，机器拉新，流量作弊等
- 目前支持安卓、IOS客户端基于TCP/UDP/HTTP/HTTPS协议的App接入（例如：手游APP、电商APP、P2P金融APP、阅读App、H5小游戏等）
- 目前暂不支持B/S架构类型的业务（例如：Web/WAP浏览器访问、微信小程序等）

玄门盾安全SDK接入

一分钟接入玄门盾，SDK目前支持Android，IOS和U3D开发环境：

1. 客户提交源站IP地址和端口号
2. 开通安全服务，告知回源IP地址，客户将回源IP地址加入源站服务器安全组（白名单）
3. 客户端调用SDK获取IP和端口，实例如下：127.0.0.1:56882

玄门盾反欺诈调用

1. 客户端初始化设备指纹
2. POST查询请求，玄门盾返回REPORT_ID，GET 对应的JSON报告

www.xmanshield.com

玄吉（上海）信息技术有限公司

上海市长宁区延安西路1319号利星行广场3楼

邮编：200041

暗号：18694842345

QQ：1064883393

微信：18694843445

电话：+86 (021) 60597859

邮箱：sales@xmanshield.com

暗号下载：

Android